STATE OF MICHIGAN
Family
Independence
Agency

MDVPTB
235 S. Grand, Suite 506
Lansing, MI 48

www.mfia.state.mi.us

Michigan Domestic Violence Prevention and Treatment Board

Tel: 517 373-8144
Fax: 517 241-8903

Memo

To: Clerk, Michigan Supreme Court

Date: Dec. 23, 2002

From: James A. Fink, Chair, Michigan Domestic Violence Prevention & Treatment Board

Subject: AO 2002-37 (Proposed Electronic Filing Standards)

In the above-referenced administrative order, the Michigan Supreme Court has requested comments regarding the kind of standards the Court should promulgate to govern electronic filing in all of Michigan's courts. Specifically, comment is requested as to whether the standards proposed by the Electronic Filing Subcommittee of the National Consortium for State Court Automation Standards ("E-filing Standards") would be suitable for implementation in Michigan.

The Integration of Court Records Has Potential to Promote the Safety of Domestic Violence Survivors

The ready access to information that is possible in today's rapidly-changing technological environment presents exciting possibilities to everyone in public service. As Chair of the Michigan Domestic Violence Prevention & Treatment Board and as a retired police officer, I applaud efforts to permit "lawyers and citizens [to] file and access documents in courts throughout the country using the same basic technological approach...." (E-filing Standards, Executive Summary, p iii.) The resulting integration of court records could enhance the safety of domestic violence survivors by allowing court and law enforcement personnel to quickly access information about criminal and protection order proceedings in other jurisdictions nationwide. I look forward to a time when protection orders issued in civil and criminal cases will be readily enforceable state- and nationwide because they are electronically filed and accessible to courts and law enforcement agencies. Universal standards for filing and accessing court documents will also assist courts to fairly and expeditiously process domestic relations matters that cross jurisdictional lines.

Unlimited Public Access to Electronic Records Poses a Potential Danger to Domestic Violence Survivors

Although electronic access to court records by court and law enforcement personnel holds promise for promoting survivor safety in cases involving domestic violence, I have concerns about public access to certain electronic records, particularly in light of the Supreme Court's

stated intent in AO 2002-37 to develop a "central data base that would be accessible to the public." A domestic violence survivor's most basic need is for physical safety. Some survivors go to great lengths to keep their whereabouts confidential from perpetrators or their agents because they are in legitimate fear for their lives. For these survivors and their children, public access to an address or telephone number could lead to harassment, abduction, physical injury, or even death. I thus urge the Court to consider the safety of domestic violence survivors and their children as it works towards public accessibility of court records.

Regarding case and document confidentiality, I note that proposed functional standard 3.7 of the E-filing Standards recognizes the necessity of providing for restrictions on public access in certain situations. However, functional standard 3.7 "does not address the confidentiality of specific data fields (e.g., address of victim) that may exist within filed documents." For guidance on this subject, functional standard 3.7 references *Public Access to Court Records: Guidelines for Policy Development by State Courts* ("Public Access Guidelines"), a document developed by the National Center for State Courts and the Justice Management Institute. These Guidelines are not mentioned in AO 2002-37, and it is not clear to what extent the Supreme Court will be considering them in implementing electronic filing procedures. Because AO 2002-37 does not mention the Public Access Guidelines, I will not make extensive comments on them here. However, some nationally-recognized domestic violence experts have commented on the practical implications of the Public Access Guidelines for the safety of survivors and their children. To illustrate the concerns raised by these experts, I have attached for the Court's information a copy of eleven "talking points" proposed by the National Network to End Domestic Violence. A few of the unanswered questions raised in this and other commentaries are:

- What costs will be associated with redacting confidential material, creating and maintaining protected access, and teaching the general public and unrepresented litigants about an electronic filing system?
- How will records be kept confidential pending a court decision on an individual's request to restrict public access to information under Section 4.70 of the Guidelines?
- If the court denies a request to restrict remote/Internet access, will this determination be made public? Will individuals whose requests are denied be allowed to privately withdraw the actions in question from the court's files if they do not wish to proceed after the court's decision?
- If a request is made to access confidential information under Section 4.70 of the Guidelines, how will the person who requested confidentiality be notified? Will that person be permitted to present oral argument, testimony, or other evidence in opposition to the request?

I urge the Court to carefully consider the comments made regarding the Public Access Guidelines as it decides what confidentiality safeguards should be incorporated into the public access provisions of any statewide electronic filing standards.

Unlimited Public Access to Court Records May Create Obstacles That Prevent Domestic Violence Survivors From Seeking or Using Available Court Services

I also encourage the Court to examine the ways in which electronic filing and remote public access might impede a domestic violence survivor's ability to use court services. Policy Standard 1.1L of the E-filing Standards correctly anticipates the physical and financial obstacles to

electronic filing that some domestic violence survivors might encounter. I support the commentary to this standard that courts should permit waivers of filing and/or access fees, and assure that computers are available for use in shelters or public facilities. Additionally, I encourage the Court to consider that survivor safety may be compromised in some cases by unlimited public access to court records, so that survivors may be reluctant to seek or use available court services. In this regard, it may not be enough to suppress identifying information only in cases directly related to domestic violence incidents, such as PPO cases. Neither the commentary to Functional Standard 3.7 of the E-filing Standards nor the confidentiality provisions of the Public Access Guidelines fully address the question of how a survivor's whereabouts might be kept confidential from perpetrators or their agents in cases that do not directly concern domestic violence. Prior to implementation of the proposed E-filing Standards, I encourage the Court to explore this question, recognizing the need to accommodate public access for legitimate purposes.

Paper Copies Have Some Safety Advantages for Domestic Violence Survivors

Finally, I have some concerns with the E-filing Standards' goal to eliminate or sharply reduce the production and use of paper copies. (See Policy Standard 1.1B and commentary.) I urge the Court to consider that domestic violence perpetrators might seek to manipulate or tamper with electronic court documents and/or to impede survivors' access to electronic court documents. These possibilities should be taken into consideration in implementing Policy Standards 1.1G and 1.1H, which require courts to authenticate the identity of persons interacting with the electronic filing system and to take steps to ensure document integrity.[1] Paper copies of certain documents (such as protection orders) may have some utility for survivors who need copies to serve on persons threatening to violate the orders, or to show or give to police called to the scene of a violation.

The MDVPTB Can Be a Resource for the Court

Electronic filing and increased remote access to court documents have a tremendous potential to benefit domestic violence survivors by streamlining court processes and making case information readily accessible to court personnel and law enforcement agencies. However, public access to court documents has the potential to adversely affect survivor safety in all types of cases. I urge the court to consider the special needs of domestic violence survivors as it contemplates action in this complex area. The Michigan Domestic Violence Prevention and Treatment Board has been working for the safety of survivors for nearly 25 years. The Board and its staff are available to share their expertise and experience with the Court during this process. Please let me know how we can assist the Court as this work progresses. We would welcome the opportunity to work with the Court on this issue.

---

[1] Attached to this memorandum is an excerpt from an article by Ann L. Kranz and Karen Nakamura, regarding batterers' use of technology to track and harass their intimate partners.

Helpful or Harmful?
How Innovative Communication Technology Affects Survivors of Intimate Violence

by Ann L. Kranz, Director of Violence Against Women Online Resources
with Karen Nakamura, Assistant Professor of Anthropology, Macalester College

May 8, 2002

Table of Contents

Author's Notes

Correspondence can be sent to:
Ann L. Kranz
Minnesota Center Against Violence and Abuse
School of Social Work, University of Minnesota
140 Peters Hall, 1404 Gortner Avenue
Saint Paul, MN 55108
Email:akranz@che.umn.edu

Karen Nakamura
Assistant Professor of Anthropology
Macalester College
1600 Grand Avenue
Saint Paul MN 55105

Special thanks to Cindy Southworth for a thorough review and instrumental edit of this manuscript.

Return to the top

Introduction

The rapid integration of both Internet and wireless technology into contemporary American culture has created both benefits and detriments for survivors of intimate violence. The Internet has provided domestic violence organizations with a greater capacity to reach out to victims of domestic violence than previously possible through print and word-of-mouth outreach efforts. It has also provided some women, albeit predominantly economically privileged women, greater access to resources about domestic violence as well as Internet based support groups. Unfortunately, Internet and wireless technologies have also aided batterers' efforts to further monitor and control their partners' activities, thereby placing battered women at risk of serious and fatal injuries. This paper explores: 1) the prevalence of web usage by both survivors of intimate violence and the organizations that serve them; 2) the ways in which batterers misuse communication technology to monitor and control their partners activities; and 3) precautions that survivors and organizations can employ to safeguard themselves from liability and harm.

Return to the top

Communication Technology Usage

For those in the United States with the economic privilege to afford it, Internet and wireless communication penetration rates have steadily increased. Today, over 168 million United States households currently have Internet access (Nielsen/Netratings, 2001) and more than 50% of households in the 25 largest U.S. cities use a wireless phone (J.D. Power and Associates, 2001). In the previous year, the percentage of consumers accessing the Internet from wireless phones doubled to 23% (J.D. Power and Associates, 2001). Internet access anytime, anywhere is the wave of the future and experts predict that by 2005, over one billion users worldwide will use the Internet (U.S. Internet Council, 2001). So, how does this rapid proliferation of innovative communication technologies impact human service delivery and specifically, the provision of advocacy and support to survivors of intimate violence?

The Internet offers new opportunities for outreach and a new arena for service delivery, which is very attractive to a movement committed to social change. While there are many advantages, domestic violence organizations should temper enthusiasm for this new medium with a critical examination of innovative communication technology usage. The foundation of the battered women's movement is to provide services that are accessible to all people so that no one is denied access. The digital divide, a term used to describe the chasm between those with and without Internet access, limits some people's access to online resources. Therefore, domestic violence organizations must learn about the digital divide (see Appendix A) in order to understand who benefits from services that involve innovative communication technologies. Domestic violence organizations should carefully weigh budget allocation decisions regarding the development or enhancement of programming. If programs devote limited financial resources to merely developing Internet-related services, they will neglect to meet the needs of all people. Further, organizations must ensure that the technologies they deploy do not further ostracize parts of the population, such as the disabled, from their services.

Return to the top

Survivors Online

There are no empirical studies documenting survivors' use of the Internet. However, by looking at studies regarding women's web usage and general rates of women's victimization, it is possible to make projections about survivors' use of the web.

Women are surfing the world-wide-web in record numbers and have surpassed men in usage, representing a little over half of the total web population (Rickert & Sacharow, 2000). The American Psychological Association (1996) suggests that one in three adult women experience at least one physical assault by a partner during adulthood. These rates of victimization also appear in teen dating relationships and same-sex couples (Barnes, 1998; Brustin, 1995). If half of the web population is female, and one-third of all women are victims of intimate violence (and it is acknowledged that this rate is consistent among teens and same-sex relationships), then it is reasonable to conclude that a significant percentage of Internet users are victims of domestic violence. With over 168 million U.S. households using the Internet, the potential number of survivors using the Internet is staggering.

Only one study to date documents online help-seeking requests from survivors of intimate violence. This study examined 427 email requests sent to Violence Against Women Online Resources, a website that delivers information on interventions to stop violence against women. Survivors of intimate violence sent in 153 (35.8%) of the total requests between October 1, 1999 and September 30, 2000. Survivors predominantly requested (66%) advocacy or crisis support (Kranz, 2001).

Return to the top

Domestic Violence Organizations Online

The Internet is a powerful medium offering many benefits to domestic violence organizations. It can break down barriers to some underserved populations, reduce costly and cumbersome outreach methods, and communicate critical communication in a timely manner.

The Internet can alleviate physical and geographic barriers causing isolation for people with mobility limitations due to disabilities, those who live in rural areas with limited support resources available to them, and those with care-giving responsibilities who are unable to leave their home. People who may otherwise be unable to access assistance can find others with similar interests and a variety of resources that may meet their needs.

The web allows for immediate posting and updating of information. Printed materials can quickly become out-of-date, leaving domestic violence organizations with large quantities of obsolete or inaccurate information. Alternatively, the web allows for changes to be made and viewed by the public instantaneously and is thereby an attractive alternative for communicating time-sensitive matters about legislation, technology, events and time-limited projects.

Jerry Finn, a leading researcher in the field of online human service delivery, has documented the surge of domestic violence material on the web. By using Hotbot, an internet search engine, Finn (2000a) found that 24,880 ".org" web pages were indexed under "family violence" and other related terms in February 1999. This represented a 37% increase in just six months.

Finn (2000b) also conducted a survey of 166 domestic violence organizations with a web site. He found that domestic violence organizations reported five main functions they hoped to achieve with their online presence: (1) agency visibility; (2) direct service; (3) community education; (4)

advocacy; and (5) securing resources (Finn, 2000). Domestic violence organizations reported the following types of direct services offered through their web presence: (1) online assessments of violent relationship; (2) outreach to survivors; (3) information and referral; (4) direct service through email; (5) links to monitored online chat rooms; (6) online support groups; and (7) art and stories by survivors (Finn 2000b).

Much more research is needed to guide domestic violence organizations' rapidly growing web presence. Finn (2000b) notes, "...there has been little empirical study of the types of services offered online or the benefits and problems encountered by human service organizations in providing these services." Technological advancements have outpaced program evaluation. However, despite the lack of empirical study, domestic violence organizations have created a growing array of resources on the web.

Return to the top

Batterers' Use of Technology

Batterers are using Internet and wireless technologies to aid their efforts to control their partners' activities by committing high-tech eavesdropping, tampering with email, monitoring home and Internet activities, and tracking the locations of their victims. No empirical studies to date have examined these misuses of technology, but advocates who work with battered women are reporting anecdotal accounts of batterers using surveillance equipment, covert web monitoring software, caller ID and other devices to locate, harass, and stalk their victims.

Cindy Southworth, a consultant who trains domestic violence advocates on technology issues, relays technology risks and victims' stories in her advocate training materials, entitled Critical Domestic Violence Advocacy, Technology and Safety Information. She details how batterers may misuse certain technologies and informs advocates how to more securely use technology and plan for safety with victims using technology (Southworth, 2001).

The following information describes some of the ways batterers can monitor their partners' communication:

- **High-tech eavesdropping**: A wireless (cellular) phone can be used as a listening device. Depending on the phone's settings, it can silently pick up sounds within its proximity. A batterer can strategically place a wireless phone in a home, car, or on someone's person and call the number throughout the day to hear conversations and activities. The phone never rings, but automatically answers. If the victim is not aware of these features, she will never know that her communication is monitored (Southworth, 2001). Certain models of corded fax and answering machines also offer this feature, although the ringing action is usually more obvious.

  Batterers may be particularly capable of monitoring the communication of a partner with a physical disability. Certain visual impairments may require a person to use large print or a software program that reads aloud text from the computer screen. Others may be able to read the large print from a distance or hear the computerized voice from a doorway or nearby cubicle without the visually impaired person knowing someone is there. Or a readily available baby monitor may be used. Other disabilities may necessitate the use of a voice-type dictation program enabling a user to speak into a microphone while the computer types the text. In these scenarios, privacy is difficult to achieve because a partner, colleague, or caregiver may see or hear a confidential conversation about a sensitive matter.

Batterers can also use a scanner to monitor communication transmitted over most brands of analog wireless or cordless phones. A well-positioned scanner in a car on the street can pick up conversations on a wireless or cordless phone in a home. Survivors should secure phone communication about sensitive matters by using a "traditional" phone with a cord that is plugged into the wall. This will ensure that a nearby scanner, baby monitor, or another cordless phone cannot pick up the signal (Southworth, 2001). If a call starts on a cordless phone and the user switches to a traditional phone, the cordless phone may continue to broadcast even after it is hung up. It is safer to unplug the cordless after switching to a traditional phone.

- **Email tampering**: It is possible for batterers to intercept or re-direct email to their account or they can program email software to place a copy of mail messages in other mailboxes. It is also easy to remotely check incoming email and leave the messages on the main email server without alerting the survivor at the home computer that the messages have already been read. Survivors may not be aware that their mail is being copied or they may not realize that the software program stores a copy of each message sent in the "Sent Items" folder. Survivors may feel they have deleted mail that has been sent or received, but have not realized that they must also empty their "deleted email folder" in order to erase any record of the correspondence. For private correspondence, it might be safest to set up a separate email account using a web-based email service such as Yahoo Mail or Hotmail. As long as the password is kept private and the automatic login feature is disabled, it is difficult to hack into these sites. Note, however, that the web browser's History Log feature will show that the email site was visited, although it won't reveal the contents. Delete the History Log if this is a matter of concern. However, if a monitoring program is running on the computer (see below), web-based mail in addition to almost all computer use, can be viewed by the abuser even if the history and temporary files are cleared.

- **Monitoring home and Internet activity**: Batterers can use web cams and other hidden surveillance cameras to monitor their partners' activities when they are away from a shared home or at their former partner's new home. Web cameras are small devices about the size of ping-pong ball that can be installed almost anywhere. Images picked up by the camera's lens can be viewed via a web page, thereby allowing abusive partners to monitor activities happening at home. Victims are often unaware that these cameras exist in their homes because they have been discreetly installed.

  Internet browsers (i.e. Netscape and Explorer) keep several histories of recent sites visited on the web. Survivors may not realize this information is automatically saved in the computer's temporary Internet file or cache file and batterers can access this file to discover where they have been online. Other software programs (i.e. Big Brother, WinGuardian, CyberPatrol, Spy Agent, and numerous others) invisibly monitor a user's activities such as web surfing, online chatting, and email exchanges. While these programs are often marketed to parents as a tool to filter and track their child's exposure to inappropriate Internet content, individuals who seek to monitor their partners' Internet communications also utilize them. These programs have the capacity to take pictures of the computer screen, record a user's ID and passwords, record both the sender and receiver's chat correspondence and incoming or outgoing mail. The software generates a report that issent over the Internet to whomever is monitoring the communication, thereby giving batterers remote access to all Internet communication.

  Newer email viruses such as the NIMDA virus allow even unsophisticated hackers to install "backdoors" into Windows systems that allow remote control of the computer. Be very careful of opening any email attachments, even if they are from people you know and trust. Run and update anti-virus software often. Other operating systems such as MacOS and Linux are much less vulnerable to back-door attacks, but if an abuser has physical or remote access to a

survivor's computer, there are many tools to monitor her computer use.

- **Tracking the location of victims**: Batterers can use features like caller ID, last number call-return, and fax headers to determine their partners' approximate location. By calling national directory assistance, one can request an operator to look up an address that correlates to a phone number. If a survivor flees to a shelter, but communicates with the batterer (or someone who shares information with the batterer), the batterer may track the location of the victim through the number listed at the head of a faxed document or from the display of a phone with caller ID. Many people are unaware that they need to enter a special code or re-program their fax in order to "block" their number from being displayed. Free caller ID "line-blocking" can be placed on regular phone lines and fax lines to prevent the phone number from appearing with caller ID.

  It is important to be very careful of calling 1-800 type "call-me" numbers. Toll-free numbers report the phone number of the caller on the phone bill, even if Caller-ID blocking is established. This is because the phone company believes that the person who is paying the bill has the right to know where the calls are coming from. The most anonymous way to call someone is to use a pre-paid telephone card purchased from a national vendor. Although these are not totally anonymous, they require much more work to track down.

  Global Positioning Software (GPS) technology is now readily available on the consumer market. Batterers can install GPS in a car for less than $300 and the system is accurate enough to tell which side of the road a car is parked. The antenna is about one-inch by one-inch and requires a clear view of the sky. Victims may not realize what this antenna does or notice it at all. Once installed, the unit logs the location, time, and speed of vehicle at all times. There have already been reports of people installing GPS units to track their teenagers' and spouses' use of the family car.

  The cellular and PCS wireless industry has been mandated by the government to develop technologies that allow emergency personnel to pinpoint the location of a person using a phone, to call 911, for example. This has already been implemented in some areas. While the current iteration only allows for 911 services to get location data, the precedence in such countries as the U.K. is for real-time and logged location information to be made available by subpoena from courts or to marketing companies who hope to provide listings of nearby businesses to the user of the phone.

Return to the top

Mitigating Risks

Primary risks of online service delivery include threats to personal safety, liability to the service provider, confidentiality breaches, lack of privacy, and ineffective service delivery (Banach and Bernat, 2000; Finn, 2001; Levine, 2000; Meier, 2000; Sampson, Jr., 2000; and Waldron, Lavitt and Kelley, 2000). Domestic violence organizations must ensure that their practices do not further endanger people they serve or the staff members providing the services. Any response made with Internet communication, faxes or phones with Caller ID has the potential to endanger the safety of a victim if intercepted or read by someone other than the victim. Recognizing the safety implication involved with such a response is the first step to creating safer organizational practices.

Safety and ethical issues involved with online service delivery and other innovative communication technologies include: a) violations of privacy; b) misunderstood communications; c) disinhibited

communication and premature intimacy; d) rapid and wide spread of inaccurate information; e) cyber-addiction; f) misrepresentation of identity; g) unanticipated and burdensome obligations; h) lack of procedures and rules; i) online harassment and stalking; and j) a lack of knowledge about technology (Waldron, Lavitt and Kelley, 2000).

These safety and ethical issues create liability issues for individual staff members, organizations, and perhaps technology developers. How should staff respond to an email message without possibly affecting a survivor's safety? If a particular organization cannot help a victim, can staff forward email to another organization that may be better suited to meet the need? Can an organization be held liable if a victim is harmed as a result of receiving help online? Can the company that developed the covert monitoring software be held liable for the damage caused to a victim who was unaware that the program was emailing reports of her Internet activity to her partner? Only one study to date specifically addresses liability issues for online service delivery by domestic violence organizations. In that study, Finn (2001) reveals that no legal precedent has been established regarding these matters.

There are a variety of practices that can be implemented on both micro- and macro-levels to mitigate problems due to innovative communication technologies. Victims, advocates, and technology developers can undertake steps to initiate protective measures and therefore safer technology usage:

- **Victims and organizations alike must first become aware of the implications involved with service delivery via innovative communication technology.** A public awareness campaign is needed at both the local and national levels. Such a campaign could involve radio, television, print and online public service announcements targeted to battered women informing them of the ways in which their communication may be monitored and suggesting safer communication alternatives.

- **Victims must recognize that their computers and wireless phones are not secure communication devices.** Victims of intimate violence should use computers that their batterers do not have direct or remote access to or if they choose to use their computer for help-seeking, they should regularly clear their many different history files, empty their trash, check for covert web software. These activities, however, do not entirely secure the communication especially from hidden monitoring programs that record all computer use. Victims should also look for installed surveillance equipment like web cams, examine the settings on their wireless phones, avoid wireless/cordless phone communication about sensitive matters, and seek local face-to-face support to deal with the effects of domestic violence. Use of public computers such as in libraries or Internet cafes and web-based email services such as Yahoo Mail or Hotmail may be safer.

- **Domestic violence organizations should develop criteria to evaluate web publishing content, especially with respect to assessment tools.** There are many resources about domestic violence on the web including red flags of abusive relationships (Domestic Abuse Project, 2001), types of abuse and warning signs (Boston University, 2001), and lethality assessment tools (VAWnet, 2001). If assessment worksheets (i.e. "Red Flags of an Abusive Relationship" and "Lethality Assessment Checklist") are normally distributed and discussed in the presence of a trained advocate/counselor, organizations should think twice before posting such content to the web. Any tool that is better delivered in the presence of a trained professional who can help interpret sensitive findings, is not appropriate for web posting (Sampson, Jr., 2000).

- **Organizations should use disclaimers on web sites, create web forms instead of "mailto" codes for email messages, draft protocol regarding online response, encourage local, face-to-face support, and not use email as a long-term advocacy tool.** Organizations should

initiate a public awareness campaign at the local level that educates battered women in their service area about the possible harmful effects and safer usage of technology.

- **Technology developers should consider product testing with battered women's advocates, holding focus groups with battered women and their advocates, consulting an attorney regarding liability, and developing a public relations campaign about their technology developments that offer "safe features" for battered women.** These PR opportunities can increase awareness and public support for their products.

- **Organizations should also be conscious that technology can limit as well as liberate.** For example, deaf victims cannot use traditional voice telephone services so counselors should be educated on how to use TTY or relay services. Web sites should be designed to be fully accessible by those with limited vision, hearing, or mobility. For example, many flashy graphic laden web sites are inaccessible for computerized text-to-speech readers for the blind; have gaudy colors that are illegible to the colorblind or visually impaired; have tiny buttons or require click-and-drag; have QuickTime movies without captions; and so forth. As with printed content material, care must be taken not to alienate based on social class, educational level, gender, race, ethnic or cultural difference.

- **The battered women's movement should develop guidelines and promising practices for online service delivery.** Once developed, a training program could be implemented to instruct advocates at the local level about safe technology practices and how to implement a local public safety campaign.

(See also Appendix B for ways to maintain privacy.)

Some people in the battered women's movement argue that the risks associated with innovative communication technologies are too great and the development of new approaches is too daunting for a movement with limited resources. While it is important to recognize the challenges, it is imperative that we do not become overwhelmed or impeded by them. Sound advice to that end can be found in the words of Mary Banach and Frances Bernat, two social work researchers:

> The practitioner should not forego using the Internet of service delivery just because the medium is still new and the method of service is still undergoing development. Protecting a client's right to confidentiality and privacy may require a practitioner to continually update her or his computer system and instruct clients and staff in their usage. The practitioner should not be discouraged in using Internet service delivery, he or she just needs to understand that their professional duties require them to consider different methods of protecting client files, records, communications, and confidences (Banach and Bernat, 2000).

Overall, it is imperative that battered women's advocates acknowledge technology issues as a critical priority and thereby designate time and resources to the cause. As a movement, we must adapt an attitude that recognizes the power of technology and the rapid proliferation that has taken place in current American culture. These new communication technologies offer many benefits to the field of domestic violence intervention and prevention. They should not be feared and avoided. Instead, they should be understood and harnessed to create positive social change.

Return to the top

References

American Psychological Association. (1996). Violence and the Family: Report of the American Psychological Association Presidential Task Force on Violence and the Family. Washington, DC.

Austen, Ian. (2000, June 29). Studies Reveal a Rush of Older Women to the Web. The New York Times, p. D7.

Banach, M. & Bernat, F. (2000). Liability and the Internet: Risks and Recommendations for Social Work Practice. Journal of Technology in Human Services. 17 (1). 153-173.

Barnes, P. (1998, February). It's Not Just A Quarrel. American Bar Association Journal. 25.

Boston University. (2001). Community Outreach Health Information System. Types of Abuse and Warning Signs. Boston, MA. .

Brustin, S. (1995). Legal Response to Teen Dating Violence. Family Law Quarterly. 29 (2). 331.

Domestic Abuse Project. (2001). Red Flags for Abusive Relationships. Minneapolis, MN. .

Finn, J. (2000a). Domestic Violence Organizations On The Web-A New Arena For Domestic Violence Services. Violence Against Women 6 (1). 80-102.

Finn, J. (2000b). A Survey Of Domestic Violence Organizations on the World Wide Web. Journal of Technology in Human Services 17 (1). 83-102.

Finn, J. (2001). Domestic Violence Organizations Online: Risks, Ethical Dilemmas, and Liability Issues. Violence Against Women Online Resources .

J.D. Power and Associates. (2001). 2001 U.S. Wireless Industry Services Study. J.D. Power Consumer Center .

Kranz, A. (2001). Survivors of Intimate Violence Seek Help Online: Implications of Responding to Increasing Requests. Violence Against Women Online Resources .

Levine, J. (2000). INTERNET: A Framework for Analyzing Online Human Service Practices. Journal of Technology in Human Services 17 (1). 173-193.

Meier, A. (2000). Offering Social Support via the Internet: A Case Study of an Online Support Group for Social Workers. Journal of Technology in Human Services 17 (1). 237-267.

Nielsen//Netratings. (2001) Global Internet Usage: Hot Off the Net. Milpitas, CA. .

Rickert, A. & Sacharow, A. (2000). It's a Woman's World Wide Web. Media Metrix, Inc. and Jupiter Communications. .

Southworth, C. (2001). Critical Domestic Violence Advocacy, Technology, and Safety Information. Harrisburg, PA.

United States Internet Council. (2001). State of the Internet 2000. Washington, DC. .

VAWnet. (2001). Lethality Assessment Tools: A Critical Analysis. Harrisburg, PA. .

Waldron, V., Lavitt, M., & Kelley, D. (2000). The Nature and Prevention of Harm in Technology-

Mediated Self-Help Settings: Three Exemplars. Journal of Technology in Human Services 17 (1). 267-295.

Return to the top

Appendix A

The digital divide is a term used to describe the chasm between those with and without Internet access. According to the United States Internet Council (2001), the divide is based on a household's annual income but is often misunderstood as a race-based disparity.

Many households cannot afford the privilege of Internet access. In a study of 200,000 web users, 78% of American households with an income over $75,000 had web access, compared to 21% of households with incomes less than $15,000 (Austen, 2000). The digital divide has segregated American citizens into "information-haves" and "have nots," leaving the nation's poor, a third of the U.S. population, out in the technological cold.

The United States Internet Council believes, however, "The U.S. should not fear a widening of the digital divide within the country. Government and industry commitments to combating the digital divide, as well as the declining costs of computers and Internet access, indicate that it will continue to narrow. Because of these efforts, many more Americans will be able to access the Internet and contribute to the closure of the digital divide" (United States Internet Council, 2001).

Return to the top

Appendix B

Ways to maintain your privacy:

- Do not use standard 80mhz or 800mhz analog cordless phones. These can be monitored quite simple. Use corded phones or cordless phones with "Digital Spread Spectrum" (DSS) technology, these are highly resistant to eavesdropping.
- Do not use standard older analog cell phones which can easily be intercepted using commercial radio scanners. The newer Sprint PCS, AT&T Digital, and other CDMA/TDMA/PCS/GSM phones are resistant to eavesdropping. Note that some "dual mode" phones may switch to analog mode depending on the area. Make sure your phone indicates when you are "analog roaming." Also note that an "all-digital network" doesn't mean the cell-phone to tower connection is necessarily digital. Make sure it says PCS, TDMA, CDMA, or GSM on the phone somewhere.
- Baby monitors and small transceivers are easy ways to monitor someone without their knowledge. Most have a limited range of 30-300 feet.
- You can ask your cell and landline telephone provider to block outgoing caller ID. However, note that the recipient of 800, 877, and 866 toll-free numbers receive the number of the caller REGARDLESS OF CALLER-ID BLOCKING STATUS. The rationale is that as the one who pays for the phone call, they should know who is calling regardless. Do not call toll-free numbers from your home phone if you do not want your number revealed. The safest way to call is from a payphone using the pre-paid telephone cards sold at gas stations, however even those records are susceptible to subpoena.
- Soon, cell-phones will be able to give location data back to the phone company as part of E-

911 services. The good news is that if someone assaults you, in the near future you only have to call 911 on your cell phone and the police will immediately know where to send a vehicle without you having to say a word. The bad news is that a hacker or a batterer with a subpoena may be able to also obtain this data.

- It is very easy to install logging software on a computer or network that tracks everything that is done, including email sent and received and web sites visited. This software is very hard to detect and circumvent. At the very least, become aware of how to clear your web browser log and how to use web-based email services such as YahooMail or Hotmail. Use public library or Internet café computers if you suspect your home computer in the least.
- Internet access to bank accounts and credit card accounts makes it easy for someone to monitor your financial transactions without your knowledge. Your bank account or credit account might be linked without your knowing it. Be sure to either use banks that are so primitive they don't have internet linking, or go ahead and create the internet bank account yourself and change the password to something that you have never used before. Many people never change their PINs and passwords, even after their divorce. Don't make that mistake.
- Answering machines, fax-answerers, and cell phones can be programmed to let the calling party enter a special code to eavesdrop on a room's conversation. If you notice your phone ring and then go silent, inspect it carefully to ensure it is not in monitoring mode.
- It is trivially easy to obtain the location of someone from their email headers, especially if they are using a home internet account. The headers will tell anyone who looks at them which "nodes" your message transferred through. Often the node will look like: smtp-relay.saint-paul.mn.company.net which will clearly indicate that you are located somewhere in the Saint Paul area. Use free anonymous web-based accounts such as Hotmail (note that privacy data from Hotmail has been uncovered by subpoena) to hide your dial-in location.
- It is also trivially easy to install a "backdoor" onto a home computer which allows someone easy access to all of your files, including email and account passwords over the Internet. Never let anyone you do not trust near your computer, even for a second. Never open email attachments, regardless of the format or sender. If you suspect your computer might be contaminated, reformat the hard drive and install applications from the original disks. Use public library or Internet café computers and free email accounts (Yahoo Mail; Hotmail) if you suspect monitoring. Macintosh and Linux computers are much less susceptible than Windows; however, even they are not totally immune.
- GPS units can be installed in hidden locations in vehicles, allowing someone to track your movements very accurately. However, GPS antennas must have a clear view of the sky so they are usually installed on the window glass, front dashboard, or back dashboard area. GPS antennas come in two varieties: square 1" x 1" flat antennas and short stubby 2" antennas. Covering the antenna with tin foil will temporarily disable it without damaging the unit.

Appendix B

Written by:
Karen Nakamura, PhD
Macalester College

Return to the top

This web site is a cooperative project of ***Office on Violence Against Women*** and ***Minnesota Center Against Violence & Abuse*** at the University of Minnesota and is supported by grant number 98-WT-VX-K001 awarded by the Office on Violence Against Women, Office of Justice Programs, U.S. Department of Justice.

Additional information about this site can be obtained by reading Email us for more information and assistance.

File Last Modified on: 8/6/02 10:38:01 AM

IV. TALKING POINTS FOR STATE & LOCAL ADVOCATES

Point to Work Towards	Explanation
A. Exclude documents in civil protection matters, family law, domestic violence, sexual assault, and stalking cases from remote or Internet access	• Public vs Published. A court may consider these cases "public" and provide access at a court facility without "publishing" them to the web. • People who have a need to look at these cases can come into the courthouse for onsite paper or electronic access. • Example: We do not want young children learning how to search the Internet in school to find their own custody or parent's divorce petitions and allegations on the Internet. • These cases do not create high volume access in the courthouse such as a large civil class action case that might have many plaintiffs and attorneys wanting remote or Internet access to reduce time at the courthouse. There is a higher likelihood that remote or Internet access would make it more convenient for people misusing this information.
B. Exclude domestic violence & sexual assault victim and witness identities from any public access	• Restrict contact information categorically (home address, phone, email) from any public access if at all possible. • Restrict remote/Internet access to names in DV, SA, stalking, family law, & protection order cases. • Allow individuals to restrict access to their names in docket listings (since many docket listings are shared widely and posted to the web).
C. Apply the access principles to all records maintained by the court including non-court records housed in the courthouse	• The Model Guidelines only apply to judicial case records, not all records maintained by court (marriage licenses, land records, etc) however some courts may automatically move to post all records housed by the courts on the Internet. A victim may relocate and need a common record filed at the court – if the land title is posted to the Internet, it will be easily searchable. • The executive branch may be responsible for non-judicial records housed in a courthouse (land records, etc). The advisory committee explained that they can't give recommendations to the executive branch however advocates can work with all branches of government to categorically or case-by-case prevent Internet access for all records.
D. Prevent the disclosure of protected information in summary court documents	• Anyone should be able to petition to restrict access in a variety of ways: file under initials or pseudonym, restrict remote or onsite access to a case -- docket number could be listed with no name and a note "case restricted or sealed", etc. • Many court systems are posting to the Internet their docket lists with summary information including name, address, docket number, case disposition, and other summary data. An online docket listing could put a victim at risk of being located by a batterer or stalker.

E. Allow any petitioner to exclude all court records from remote access	• Any citizen should be able to petition the court to restrict access in a variety of ways: file under initials or pseudonym, restrict remote or onsite access to a case -- docket number could be listed with no name and a note "case restricted or sealed", only summary information on the web not the actual documents, etc. • Many citizens including survivors of DV, SA, and stalking may have legitimate concerns about their information being posted by the courts to the Internet. Since the court can choose to provide access within the courthouse, anyone should be able to petition the court to restrict remote access. Since this is not the same as sealing a case completely, a lower standard may apply. *(These talking points are not providing legal advice, please work with attorneys in your state)*
F. Information must be protected from the time of request through decision of the court	• If someone petitions the court to either completely seal a case or restrict remote/Internet access (see D. above) their case and all information about it should be protected from the time of the request until a decision is made. • If the court posts a case to the web while the request to restrict Internet access is pending judicial review, then a victim's privacy and safety could be violated. If there is no protection of the information while a request is being reviewed, than many victims may need to choose to NOT USE THE COURT – for anything. • The advisory committee discussed this issue and initially agreed to put it in black letter of policy as long as it also recommended a reasonably quick determination by a judge so as not to leave things sealed indefinitely with no judicial determination – however this may not have made it into the printed "Model Guidelines".
G. If court denies a request to seal or restrict remote/Internet access, a victim must be able to remove her court documents without her papers being posted to the Internet. In some cases, victims might choose safety/privacy over using the court system.	• If a petition to restrict access is denied, then a victim must have the ability to withdraw her initial filing without her petition to withdraw being posted to the web. • An advisory committee member was concerned about a victim wanting to file a case at the same time as a petition to restrict access. The committee member preferred that petitioners file the petition to restrict access with the other court action (protection order perhaps) in an envelope. If the petition to restrict access is granted, then the protection order document could be officially filed with the court. Unfortunately this process may be logistically problematic for victims filing a protection order. The very nature of the case requires a quick response from the courts.

H. Permit local courts to adopt more restrictive access policies than the National Model "Guidelines"	• The February 2002 proposed Model Policy encouraged states to prohibit local courts from having more restrictive access policies than the state uniformly adopts. NNEDV believes this is counterproductive in a state where the uniform policy is harmful to victims and a local court is receptive to protecting victim information. • Local courts should have the latitude to protect the privacy and safety of their constituents. State courts might want to set a minimum level of privacy so that local courts don't post too much information to the Internet, but should not tell local courts that they must post as much private data as a less conscientious court jurisdiction.
I. Provide robust notification of electronic record management to litigants, victims, witnesses, and the community, including victim advocacy groups	• Any court contemplating increasing access to court records MUST provide robust notice on where the records are posted AND also how to restrict access. • Comprehensive notice is required by many comparable data privacy issues. (Amy Bushyeager from Mintz Levin, NNEDV's legal counsel, explained this in great detail during the NNEDV public testimony for the advisory committee.) • Some committee members were hesitant to include notice on how to restrict access for fear that a) all who use the court will petition for restriction and b) witnesses and victims might not participate in hearings if they understand that information about them will be posted to the Internet. • Some committee members were also worried about an increase in workload to provide notice to all victims, witnesses, litigants, etc. Well posted signs throughout the courthouse could assist in this notice, as could a brochure to give to witnesses when they are called to the court since frequently court administrators do not know witnesses identities prior to a hearing. Other officers of the court (prosecutors, etc) can also provide comprehensive notice to victims and witnesses. • Courts should be instructed to work with local and state victim advocacy groups (and other groups) if they are contemplating increasing access to sensitive court records and data through the Internet or other electronic means. State coalitions and local programs can assist victims in navigating the petitions to restrict access and safety planning about potential consequences of using court systems that post victim data. • Also, notice for pro se litigants is critical. Many on the committee assumed that attorneys would notify litigants. Victims, witnesses, and pro se litigants need effective notice.

J. Include processes for preventing and remedying failures to properly exclude information from public access	• All good technology initiatives include quality assurance and auditing processes. Courts must include a comprehensive and timely process PRIOR to posting any court records into an electronic system connected to the Web. • Preferably, an outside neutral office should assist or oversee an audit process to check for errors. Random sampling of all cases and checking cases where restrictions to access were granted would help identify if the court is posting information to the Internet in error. State Courts could oversee an audit process of local courts. Alternatively or in addition, an office in the court that is not responsible for the day-to-day management of the electronic court records could oversee an audit. • Since it can be assumed that errors will occur, a timely remedy process should be developed prior to implementing an electronic system. Depending on the nature of the error (posted a case to the Internet that was not supposed to be posted at all or an error within a court document) the court might want judicial review – however it should be timely. Victim safety and citizen privacy could be compromised by an error and due to Internet Search engines, selling court data in bulk, and Internet Archives, time is of the essence. Search engines index information 24hours per day – even if the error is corrected, a search engine or Web Archival site might have saved the incorrect or dangerous record. • All court staff including judges should be required to participate in training on any electronic system to reduce errors and assist in granting petitioners appropriate restrictions of Internet access. All court staff should know the process to request a restriction of access and also the process to remedy an error, even if that process is the correct referral to the appropriate staff person.
K. If the court includes a process to request that sealed or restricted information be unsealed or posted to the Internet, notice to victims and all other named parties – except batterers should be included	• The media representatives wanted the Guidelines to address unrestricting court records that had previously been restricted or sealed. It is critical to notify a victim that there is an attempt to post her sealed records on the Web. • The Guidelines also reference VAWA 2000 since it prevents courts from notifying defendants if a victim registers an out-of-state protection order. In the guidelines, the terminology "notify all parties" could confuse court staff, causing them to notify a batterer if a request to restrict or unrestrict access to a protection order is received.